App Store Monitoring

Fake or unauthorized apps threaten brand, business and customer

Digital businesses big and small rely on customer-facing apps as platforms for sales, support and customer experiences. Fraudsters and scammers recognize these apps as an opportunity to syphon from reputable online brands, defrauding business and customer. In some cases, it's brand and trademark infringement with fraudsters engaging in unauthorized distribution of branded apps. In other cases, it's fake apps or malware-laced apps aimed at stealing credentials. And in yet other instances, it's scam sites, hosting fake or malicious apps. Whatever the case, the effects can be damaging and lasting to brand reputation and trust.

Use Bolster to detect and take down fake apps and scam sites in real-time

With Bolster App Store Monitoring, you'll get immediate visibility and control. Our next-generation fraud prevention platform and trained experts will actively monitor major app stores and 3rd party app stores, over 500 in all, for unauthorized distributions and fakes apps impersonating your brand. The system will also apply deep learning and natural language processing to scour the Internet for app-related scam sites aimed at phishing credential theft.

Upon detection, our systems will automatically collect comprehensive evidence of brand and trademark infringement and phishing credential theft used to then trigger complete fully-automated takedown and removal processes. We'll ensure that fake or unauthorized apps are taken down and stay down. And for app-related scam sites or phishing credential sites detected, evidence will automatically be sent to global block lists in 6.5 seconds and full site takedowns will occur in as little as 2 minutes.

AI-Driven Detection

Real-time AI-driven detection of fake & unauthorized apps across all major app stores & 3rd party app stores, 500+ total.

Fully-Automated Takedowns

Automatically remove unauthorized or fake apps & take down scam sites globally in as little as 2 minutes.

Continuous Monitoring

Ensure that apps & sites that are taken down stay down through continuous monitoring of app stores & web sites.

Rich Threat Intelligence & Dashboarding

Intuitive dashboards & rich threat intelligence allow Brand, Legal & Security team to effectively collaborate on cases.

BOLSTER
NEXT GENERATION
Fraud Prevention Platform

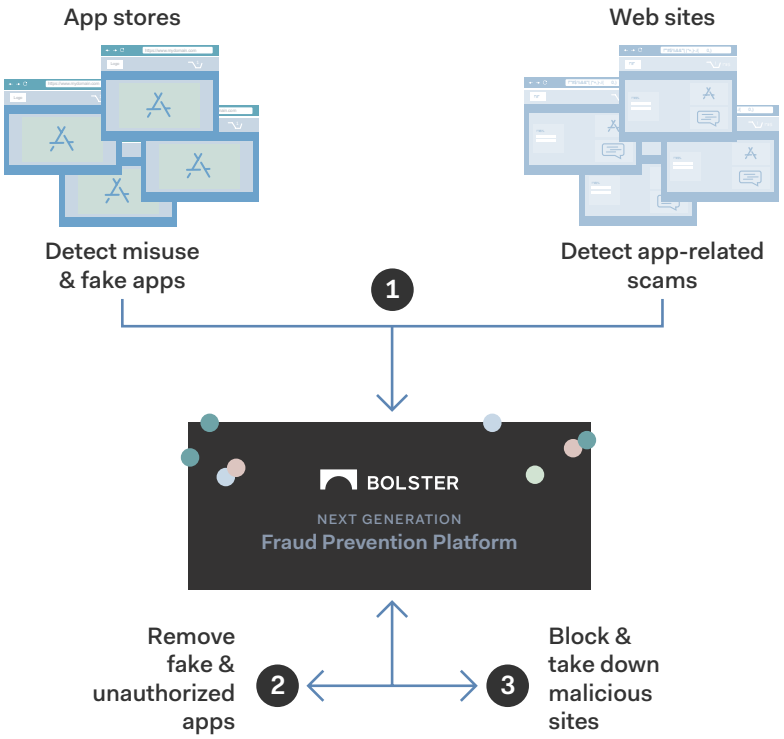
Unmatched detection & takedown capabilities keep your brand & business safe all the time.

Ultra-fast, Ultra-accurate Detection	**<100ms** Fraud detection verdict	**1/100,000** False-positive rate	**60 sec** Mean Time to Response (MTTR)
Fully-automated Zero-touch Takedowns	**2 mins** Avg API based takedown time	**95%** Without manual intervention	**6.5 sec** Submission to global blocklists

How it Works:

- Monitor all major & 3rd party app stores for unauthorized distributions & fake apps
- Detect app-related scam sites in real-time with detailed, actionable insights
- Remove fake apps, stop unauthorized distribution & sale of branded apps
- Use API & automated evidence based submissions to hosting providers & registries to take down scam sites
- Continuously monitor apps stores & Internet for re-emergence of unauthorized distributions, fake apps & scam sites

Detect & remove unauthorized or fake apps, take down app-related scam sites



AI-driven smarts from detection to takedown

Protecting Leading Brands Around the World

Booking.com · Dropbox · change.org · fitbit · LinkedIn · twilio · Uber · zoom

About

Bolster builds AI/ML technology to protect regular citizens from bad actors on the internet. Your favorite brands from technology to eCommerce trust our platform to detect and takedown threats that might attack their customers, employees, or partners.
Learn more at: www.bolster.ai

4966 El Camino Real, Suite #101
Los Altos, CA, USA 94022
info@bolster.ai